REMARKS

This Application has been carefully reviewed in light of the Final Office Action mailed March 3, 2006. Applicant appreciates the Examiner's consideration of the Application.

In order to advance prosecution of this Application, Applicant has responded to each notation by the Examiner. Applicant respectfully requests reconsideration and favorable action in this case.

Amendments

Claims 1, 2, 7-12, and 17-18 have been amended to correct informalities pointed out by the Examiner. Applicant thanks the Examiner for pointing out the informalities.

Applicant believes that the amendments place the case in condition for allowance or in better condition for appeal, do not raise the issue of new matter, and do not present new issues requiring further consideration or search. Accordingly, Applicant respectfully requests that the Examiner enter the amendments.

Section 101 Rejection

Claims 17-18 have been amended to correct an informality pointed out by the Examiner. Applicant thanks the Examiner for pointing out the informality. Accordingly, Claims 1, 2, 7-12, and 17-18 are allowable under Section 101.

Section 112 Rejection

Claims 1, 2, 7-12, and 17-18 have been amended to correct an informality pointed out by the Examiner. Applicant thanks the Examiner for pointing out the informality. Accordingly, Claims 1, 2, 7-12, and 17-18 are allowable under Section 112.

Section 103 Rejection

The Examiner rejects under 35 U.S.C. § 103(a): Claims 1-4, 6-14, and 16-18 as being unpatentable over U.S. Patent No. 6,357,008 to Nachenberg ("*Nachenberg I*") in view of U.S. Patent No. 6,453,345 to Trcka ("*Trcka*"); and Claims 5 and 15 as being unpatentable over *Nachenberg I* in view of *Trcka* and U.S. Patent No. 6,971,019 to Nachenberg

("*Nachenberg II*"). Applicant respectfully traverses this rejection for the reasons discussed below.

Applicant respectfully submits that the combinations of *Nachenberg I*, *Trcka*, and *Nachenberg II* proposed by the Examiner fail to disclose, teach, or suggest the elements of Claims 1-18. For example, *Nachenberg I-Trcka* combination proposed by the Examiner fails to disclose, teach, or suggest "triggering a viral detection alarm in response to determining that one of the listed memory regions is larger than the predetermined size," recited Claim 2.

First, *Nachenberg I* fails to disclose, teach, or suggest the element. *Nachenberg I* discloses detecting computer viruses ***based on suspicious behavior***. According to *Nachenberg I*:

> [The method comprises] three phases: a decryption phase, an exploration phase, and an evaluation phase. A purpose of the decryption phase is to emulate a sufficient number of instructions to allow an encrypted virus to decrypt its viral body. A purpose of the exploration phase is to emulate at least once all sections of code within a region deemed likely to contain any virus present in the target program. ***A purpose of the evaluation phase is to analyze any suspicious behavior observed during the decryption and exploration phases to determine whether the target appears to be infected***.

(*Nachenberg I*, Abstract, emphasis added.) That is, the *Nachenberg I* method ***analyzes suspicious behavior*** to detect computer viruses.

Nachenberg I discloses establishing whether a region of a certain size has been decrypted in order to determine when to move from the decryption phase. According to *Nachenberg I*:

> On the other hand, if the first threshold number has been reached, then the decryption module 152 determines in a fourth procedure 308 whether a region of a certain minimum size or larger appears to have been decrypted. ... ***If no such region appears to have been decrypted***, then under the assumption that any virus present is unlikely to be an encrypted virus, ***the decryption phase 252 ends*** and the exploration phase 254 begins.
>
> On the other hand, ***if such a region appears to have been decrypted***, then emulation in ***the decryption phase 252 continues*** to allow further decryption by fetching the instruction at the virtual CS:IP in the sixth procedure 312 unless a second threshold number of emulated instructions has been reached.

(*Nachenberg I*, column 8, lines 1-19, emphasis added.) That is, *Nachenberg I* establishes whether a region of a certain size has been decrypted merely to determine when to move from the decryption phase, ***but not to detect computer viruses***.

In summary, *Nachenberg I* detects computer viruses ***based on suspicious behavior, but not based on establishing whether a region of a certain size has been decrypted.*** Presumably, if the *Nachenberg I* method triggered an alarm, the alarm would be triggered in response to ***detecting suspicious behavior***, but not in response to establishing whether a region of a certain size has been decrypted. Accordingly, *Nachenberg I* fails to disclose, teach, or suggest "triggering a viral detection alarm in response to determining that one of the listed memory regions is larger than the predetermined size," as recited Claim 2.

Second, *Trcka* fails to disclose, teach, or suggest the element. *Trcka* discloses an automated monitor application. According to *Trcka*:

> The Automated Monitor application 140 uses known data processing techniques (virus checking, transaction monitoring, etc.) to automatically check for and track suspect network events. In one configuration option, the Automated Monitor 140 checks all inbound transfers of executable files for known viruses. By selecting an ALERT MONITOR menu option on the graphical user interface 104, the user can enable and disable various visual and audible event alarms. For example, the user can configure the Automated Monitor 140 to trigger an audible or visual alarm upon detecting a virus in an inbound file transfer.

(*Trcka*, column 17, lines 24-34.) That is, *Trcka* merely discloses triggering an alarm upon detecting a known virus. *Trcka*, however, fails to disclose, teach, or suggest "triggering a viral detection alarm in response to determining that one of the listed memory regions is larger than the predetermined size," as recited Claim 2.

Consequently, *Nachenberg I-Trcka* combination fails to disclose, teach, or suggest "triggering a viral detection alarm in response to determining that one of the listed memory regions is larger than the predetermined size," recited Claim 2. Accordingly, Claim 2 is allowable over the *Nachenberg I-Trcka* combination.

Independent Claims 1, 7-12, and 17-18 recite certain limitations substantially similar to those recited in independent Claim 2. Accordingly, for at least similar reasons, Claims 1, 7-12, and 17-18 are allowable over the *Nachenberg I-Trcka* combination.

Applicant respectfully requests reconsideration and allowance of independent Claims 1, 2, 7-12, and 17-18, and their dependent claims.

CONCLUSION

Applicant has made an earnest attempt to place this case in condition for allowance. For at least the foregoing reasons, Applicant respectfully requests full allowance of all the pending claims.

If the Examiner believes a telephone conference would advance prosecution of this case in any way, the Examiner is invited to contact Keiko Ichiye, the Attorney for Applicant, at the Examiner's convenience at (214) 953-6494.

Although Applicant believes no fees are due, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicant

Keiko Ichiye
Reg. No. 45,460

KI/ls

Correspondence Address:
Baker Botts L.L.P.
2001 Ross Avenue, Suite 600
Dallas, Texas 75201-2980
(214) 953-6494
Date: April 25, 2006

Customer Number: 05073